UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/557,628	11/17/2005	Pim Theo Tuyls	NL030552	4463

24737   7590   02/11/2009
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER
SIMS, JING F

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
02/11/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/557,628	TUYLS ET AL.
	Examiner	Art Unit
	JING SIMS	2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _21 November 2008_.
2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1-18_ is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a)☐ All   b)☐ Some * c)☐ None of:
   1.☐ Certified copies of the priority documents have been received.
   2.☐ Certified copies of the priority documents have been received in Application No. _____.
   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

1.   This Office action is responsive to applicant's amendment filed on November

21ˢᵗ, 2008.

2.   Claims 1-18 are amended.

3.   Applicant's arguments, with respect to claims 1-18, have been fully considered,

but they are not persuasive.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5.   **Claim 17** is rejected under 35 U.S.C. 102 (b) as being anticipated by Yamaguchi

et al (US 6314196) (hereinafter Yamaguchi).

        As per **claim 17**, Yamaguchi discloses "a system for authenticating a physical

object" (column 17, line 3-4, Yamaguchi discloses "the embodiment of a fingerprint

checking device") "the system including an enrollment device" (Figure 1, reference

number 1 Yamaguchi discloses as "image pickup unit"); "an authentication device"

(Figure 1, reference number 1, Yamaguchi discloses as "image pickup unit". The

specification of the instant application discloses that the authentication may in principle

be done using the same apparatus as used for the enrollment, therefore, authentication

device also can be "image pickup unit") "and a storage for storing authentication data"

(Figure 1, reference unit 6, Yamaguchi discloses as "registering unit", it also can be find

in Figure 20, reference number A3, Yamaguchi discloses as "temporary fingerprint

registering") "the enrollment device including: an input for receiving a property set Y of

the object measured using a measurement procedure" (Figure 1, reference number 1,

fingerprint image pickup unit); "a processor for creating a property set I from the

measured property set Y that meet a predetermined robustness criterion" (Figure 1,

reference 10, property set I appears to be the data that after binarized image converting

unit process, and the robustness criterion appears to be the control variables m or/and n

in column 4, line 52-61), "creating a property set A from the property set I that includes

less information on the actual properties than property set Y" (property set A appears to

be the data after thinning unit in figure 1. Figure 32 A to B shows the actually thing

process of a finger print. Figure 32 B, the after thinning process picture includes less

information than figure 32 A), "wherein the creating the property set I and the property

set A are guided by a criteria W" (column 4, line 52-61, and figure 1, the block number

control variables m and n control the binarized image converting and, thereafter, the

thinning process); "and generating a control value V in dependence on properties of the

property set A and the criteria W" (Figure 2, reference number A12, control value V

appears to be the best finger selection. The best fingerprint selection are based on

result after thinning process and binarized image converting, which where the m and/or

n take control to process the input fingerprint), "an output for supplying the control value

V to the storage as part of the authentication data" (Figure 2, reference number A7,

formal registering. It means the best finger print has been stored as authentication data

for future; and in and figure 17, reference number A11, store registered fingerprint data

in file for future fingerprint check as described in figure 18); "the authentication device

including: an input for receiving a property set Y' of the object measured using a

measurement procedure and for receiving the control value V from the storage including

the criteria W; a processor for creating a property set I' from the measured property set

Y' that meet a predetermined robustness criterion; for creating a property set A' from the

property set I' that includes less information on the actual properties than property set

Y', wherein the creating the property set I' and the property set A' are guided by the

criteria W; for generating a control value V' in dependence on properties of the property

set A'" (since the specification of the instant application discloses that the authentication

may in principle be done using the same apparatus as used for the enrollment,

therefore, see the rejection to claims 1 or 15, for the corresponding sections); "for

authenticating the physical object if there is a predetermined correspondence between

the generated a control value V' and the retrieved control value V and an output for

issuing a signal indicating whether or not the physical object has been authenticated"

(Figure 1, reference 5, "checking unit" and/or "judging unit"; figure 20, reference number

A5, the issued signal appears to be the signal after the process of match).

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.   **Claims 1-6, 14, 15, 16 and 18** are rejected under 35 U.S.C 103(a) as being unpatentable over Yamaguchi, in view of Kobayashi (US Patent 7093131 B1).

As per **claim 1**, Yamaguchi discloses "a method of generating authentication data for authenticating a physical object; the method comprising acts of" (column 1, line 7-8, "a fingerprint registering method for registering a fingerprint" which has the same meaning of "generating authentication data", and column 1, line 32-33 "to authenticate personal identification") "measuring a property set Y of the object using a measurement procedure" (Figure 1, reference number 1, Yamaguchi discloses this limitation as "fingerprint image pickup unit" a fingerprint image is property set, and the pickup unit certainly performing a measurement procedure to pickup the fingerprint); "creating a property set I from the measured property set Y that meet a predetermined robustness criterion" (Figure 1, reference 10, property set I appears to be the data that after binarized image converting unit process, and the robustness criterion appears to be the control variables m or/and n in column 4, line 52-61) "creating a property set A from the property set I that includes less information on the actual properties than property set Y" (property set A appears to be the data after thinning unit in figure 1. Figure 32 A to B shows the actually thing process of a finger print. Figure 32 B, the after thinning process picture includes less information than figure 32 A), "wherein the creating acts are guided by a criteria W" (column 4, line 27-33, and line 52-61, Figure

36. Yamaguchi discloses the creating acts are guided by a criteria W as m or/and n. M and n control the selection of the subsets which are the divided image blocks. Thereby limit the range of parameters (finger print pattern) which is the criteria that guides the creating acts); "generating a control value V in dependence on properties of property set A (Figure 2, reference number A12, control value V appears to be the best finger selection. The best fingerprint selection is based on result after thinning).

However Yamaguchi does not explicitly disclose "inserting the control value V and the criteria W in the authentication data".

Kobayashi discloses "inserting the control value V and the criteria W in the authentication data" (column 16, line 42-49, and Fig. 3, S118-120, control value V appears to be the authentication information generated after step S116; the criteria W appears to be the generated inspection information after step S118. Kobayashi discloses inspection information for inspecting as to whether or not an error is contained in the digital data is generated. It sets criteria for the authentication data. Kobayashi also discloses the inspection information is added as further authenticating information to the digital data).

Yamaguchi and Kobayashi are analogous art because they are from the same field of endeavor of a method and apparatus for processing and authenticating input information.

Therefore, it would have been obvious to one of ordinary skill in the art at the invention of time to modify the teaching of Yamaguchi to generate a authentication data, which in this case are finger prints, that selected by criteria factors m and n, and add the

selecting criteria to the authentication information, same as the inspection information

that are added to its digital data as authentication information that taught by Kobayashi

because therefore the data should be free from alteration and have objectivity, and to

improve the probative value of data as evidence (see Kobayashi page2, line 10-13).

As per **claim 2**, Yamaguchi discloses "the method as claimed in claim 1, wherein

the act of creating the property set A includes performing a contracting transformation

that transforms given ranges of input properties to corresponding output values" (Figure

3, reference number B4, Yamaguchi discloses as "extract minutiae". The process of

"extracting minutiae" is to transform a biometric data - for example a fingerprint - from

one state to the other state by performing "extract minutiae". The input properties range

is the thinning processed image and the output values are the minutiae are the detected

minutia based on the thinning processed image in column 20, line 61-63,).

As per **claim 3**, Yamaguchi discloses "the method as claimed in claim 1, wherein

the contracting transformation transforms a property to a binary number representative

of whether the property has a positive or negative value" (Figure 17, reference number

A8, and column 29, line 7-8 "the content d at the n-th byte of the registered fingerprint

data is stored in the register (A8)" Yamaguchi discloses the content in "byte", it is the

length unit used by binary numbers, therefore, "a property" is represented by binary

numbers. Transforming a property to binary number representative of whether the

property has a positive or negative value is well known technology in the art, for

example, US Patent 3,947,876 discloses "to convert the positive and negative data

transitions to binary ones and zeros respectively" (see Gary, column 7, line 50-54)).

As per **claim 4**, Yamaguchi discloses "the method as claimed in claim 1, wherein the act of creating the property set A includes an act of selecting a subset of the property set I" (column 4, line 27-30 and line 52-61, Yamaguchi discloses an self-explanatory diagram in Figure 36, Yamaguchi also explains "dividing a pictured image into blocks, and when 512.times.512 picture elements are determined as one screen, division into 1024 blocks is made with 16.times.16 picture elements as one block"; therefore, the blocks have the equal meaning with "subsets" in the instant application. Yamaguchi further discloses "selecting a subset" as in Figure 38, and give the example of "the flowchart of a conventional example". It is an actually selecting process of subsets in Yamaguchi's application).

As per **claim 5**, Yamaguchi discloses "the method as claimed in claim 4, including an act of creating criteria W for controlling the selection" (column 4, line 27-33, and line 52-61, Figure 36 are an self-explanatory diagram of dividing a pictured image into blocks, the subset has been described as blocks "in which a block number is initialized with m=1 (B-1). In other words, number m for 1 to 1024 is allocated with respect to 1024 blocks in the image shown in FIG. 36, and the block number m is determined as 1 for initialization. Then, with n=1 (B2), the picture element number n in the block is initialized. In other words, the number n for 256 picture elements in the image shown in FIG. 36 is allocated, and this picture element number n is determined as 1 for initialization." Yamaguchi discloses the "criteria W" in the application appears to be m or/and n. M and n controls the selection of the subsets which are the divided

image blocks. Thereby limit the range of parameters (finger print pattern) which is the criteria that controls the selection).

As per **claim 6**, Yamaguchi discloses "the method as claimed in claim 5, including an act of creating unique criteria W based on respective authentication applications" (column 3, line 57-67, Yamaguchi discloses "based on the multivalued image, it is judged by the fingerprinting judging unit 313" "division into respective blocks is made". Yamaguchi discloses earlier "block number m and picture element number n", so m is block number. It indicates from above statements that the block number m is based on the multivalued image. The multivalued image is generated upon the fingerprint by the fingerprint image pickup unit 311. Therefore, the block number m is uniquely created respect to each authentication applications), "wherein different respective authentication applications have different unique criteria" (m and n are variables. The example in col. 4, line 52-61, m has been set to 1-1024, and n has been set to 1-256; however, Yamaguchi also discloses the criteria can be changed due to different applications in col. 4, line 5-8, as the process of determining the luminance of the focused picture element can be made with respect to blocks. In col. 3, line 64-67, it indicates the block can be 16x16 or others, which indicates the criteria/variables m and n may be changed based on the luminance of each application).

As per **claim 14**, Yamaguchi discloses "a computer program stored on a computer readable memory device for generating authentication data for authenticating a physical object, the computer program being operative to cause a processor to" (Figure 45, and column 10, line 7-15, the fingerprint checking device includes a

processor, a read-only memory storing a program, a multivalued image memory, a

binarized image memory): "measure a property set Y of the object using a

measurement procedure" (Figure 1, reference number 1, Yamaguchi discloses this

limitation as "fingerprint image pickup unit" a fingerprint image is property set, and the

pickup unit certainly performing a measurement procedure to pickup the fingerprint);

"create a property set I from the measured property set Y that meet a predetermined

robustness criterion" (Figure 1, reference 10, property set I appears to be the data that

after binarized image converting unit process, and the robustness criterion appears to

be the control variables m or/and n in column 4, line 52-61) "create a property set A

from the property set I that includes less information on the actual properties than

property set Y" (property set A appears to be the data after thinning unit in figure 1.

Figure 32 A to B shows the actually thing process of a finger print. Figure 32 B, the

after thinning process picture includes less information than figure 32 A), "wherein the

creating acts are guided by a criteria W" (column 4, line 27-33, and line 52-61, Figure

36. Yamaguchi discloses the creating acts are guided by a criteria W as m or/and n. M

and n control the selection of the subsets which are the divided image blocks. Thereby

limit the range of parameters (finger print pattern) which is the criteria that guides the

creating acts); "generate a control value V in dependence on properties of property set

A (Figure 2, reference number A12, control value V appears to be the best finger

selection. The best fingerprint selection is based on result after thinning).

However, Yamaguchi does not explicitly disclose "inserting the control value V

and the criteria W in the authentication data".

Kobayashi discloses "insert the control value V and the criteria W in the

authentication data" (column 16, line 42-49, and Fig. 3, S118-120, control value V

appears to be the authentication information generated after step S116; the criteria W

appears to be the generated inspection information after step S118. Kobayashi

discloses inspection information for inspecting as to whether or not an error is contained

in the digital data is generated. It sets criteria for the authentication data. Kobayashi

also discloses the inspection information is added as further authenticating information

to the digital data).

Yamaguchi and Kobayashi are analogous art because they are from the same

field of endeavor of a method and apparatus for processing and authenticating input

information.

Therefore, it would have been obvious to one of ordinary skill in the art at the

invention of time to modify the teaching of Yamaguchi to generate a authentication data,

which in this case are finger prints, that selected by criteria factors m and n, and add the

selecting criteria to the authentication information, same as the inspection information

that are added to its digital data as authentication information that taught by Kobayashi

because therefore the data should be free from alteration and have objectivity, and to

improve the probative value of data as evidence (see Kobayashi page2, line 10-13).

As per **claim 15**, Yamaguchi discloses "a method of authenticating a physical

object; the method comprising acts of : measuring a property set Y of the object using a

measurement procedure; creating a property set I from the measured property set Y

that meet a predetermined robustness criterion; creating a property set A from the

property set I that includes less information on the actual properties than property set Y;

generating a control value V' in dependence on properties of the property set A". The

limitations above are identical to a method of generating authentication data in claim 1.

To avoid redundancy, all the rejection for claim 1 is also applied to the part of claim 15

above. Yamaguchi also discloses "retrieving a control value V that has been generated

for the physical object during an enrollment; and authenticating the physical object if

there is a predetermined correspondence between the generated control value V' and

the retrieved control value V" (column 30, line 25-35, in Fig. 20, flowchart of registering

of the register "first fingerprint" in reference number A2, and by authenticating the

physical object by "match" in reference number A5. "The first fingerprinting is effected"

means the process of retrieving a control value V. "A predetermined correspondence"

are explained as "to judge whether or not they match" in prior art. It discloses "the

authentication may in principle be done using the same apparatus as used for the

enrollment" in the specification. Fig. 20 in Yamaguchi's application is the example of

this model); however Yamaguchi does not explicitly disclose "retrieving a control value

V including a criteria W, wherein the creating acts are guided by the criteria W".

Kobayashi discloses "inserting the control value V and the criteria W in the

authentication data" (column 16, line 42-49, and Fig. 3, S118-120, control value V

appears to be the authentication information generated after step S116; the criteria W

appears to be the generated inspection information after step S118. Kobayashi

discloses inspection information for inspecting as to whether or not an error is contained

in the digital data is generated. It sets criteria for the authentication data. Kobayashi

also discloses the inspection information is added as further authenticating information to the digital data), therefore, if the criteria W has been inserted to authentication data as described above, when retrieving process retrieves "first fingerprint" the inserted criteria would be retrieved all together.

Yamaguchi and Kobayashi are analogous art because they are from the same field of endeavor of a method and apparatus for processing and authenticating input information.

Therefore, it would have been obvious to one of ordinary skill in the art at the invention of time to modify the teaching of Yamaguchi to generate a authentication data, which in this case are finger prints, that selected by criteria factors m and n, and add the selecting criteria to the authentication information, same as the inspection information that are added to its digital data as authentication information that taught by Kobayashi because therefore the data should be free from alteration and have objectivity, and to improve the probative value of data as evidence (see Kobayashi page2, line 10-13).

As per **claim 16**, Yamaguchi discloses "a computer program stored on a computer readable memory device for authenticating a physical object, the computer program being operative to cause a processor to" (Figure 45, and column 10, line 7-15, the fingerprint checking device includes a processor, a read-only memory storing a program, a multivalued image memory, a binarized image memory): "measure a property set Y of the object using a measurement procedure" (Figure 1, reference number 1, Yamaguchi discloses this limitation as "fingerprint image pickup unit" a fingerprint image is property set, and the pickup unit certainly performing a

measurement procedure to pickup the fingerprint); "create a property set I from the

measured property set Y that meet a predetermined robustness criterion" (Figure 1,

reference 10, property set I appears to be the data that after binarized image converting

unit process, and the robustness criterion appears to be the control variables m or/and n

in column 4, line 52-61) "create a property set A from the property set I that includes

less information on the actual properties than property set Y" (property set A appears to

be the data after thinning unit in figure 1. Figure 32 A to B shows the actually thing

process of a finger print. Figure 32 B, the after thinning process picture includes less

information than figure 32 A), "generate a control value V in dependence on properties

of property set A (Figure 2, reference number A12, control value V appears to be the

best finger selection. The best fingerprint selection is based on result after thinning),

"generating a control value V' in dependence on properties of property set A (Figure 2,

reference number A12, control value V appears to be the best finger selection. The

best fingerprint selection is based on result after thinning. The specification of the

instant application discloses that the authentication may in principle be done using the

same apparatus as used for the enrollment), "retrieving a control value V that has been

generated for the physical object during an enrollment; and authenticating the physical

object if there is a predetermined correspondence between the generated control value

V' and the retrieved control value V" (column 30, line 25-35, in Fig. 20, flowchart of

registering of the register "first fingerprint" in reference number A2, and by

authenticating the physical object by "match" in reference number A5. "The first

fingerprinting is effected" means the process of retrieving a control value V. "A

predetermined correspondence" are explained as "to judge whether or not they match"

in prior art. It discloses "the authentication may in principle be done using the same

apparatus as used for the enrollment" in the specification. Fig. 20 in Yamaguchi's

application is the example of this model); however, Yamaguchi does not explicitly

disclose "retrieving a control value V including a criteria W, wherein the creating acts

are guided by the criteria W".

Kobayashi discloses "inserting the control value V and the criteria W in the

authentication data" (column 16, line 42-49, and Fig. 3, S118-120, control value V

appears to be the authentication information generated after step S116; the criteria W

appears to be the generated inspection information after step S118. Kobayashi

discloses inspection information for inspecting as to whether or not an error is contained

in the digital data is generated. It sets criteria for the authentication data. Kobayashi

also discloses the inspection information is added as further authenticating information

to the digital data), therefore, if the criteria W has been inserted to authentication data

as described above, when retrieving process retrieves "first fingerprint" the inserted

criteria would be retrieved all together.

However, Yamaguchi does not explicitly disclose "inserting the control value V

and the criteria W in the authentication data".

Kobayashi discloses "insert the control value V and the criteria W in the

authentication data" (column 16, line 42-49, and Fig. 3, S118-120, control value V

appears to be the authentication information generated after step S116; the criteria W

appears to be the generated inspection information after step S118. Kobayashi

discloses inspection information for inspecting as to whether or not an error is contained

in the digital data is generated. It sets criteria for the authentication data. Kobayashi

also discloses the inspection information is added as further authenticating information

to the digital data).

Yamaguchi and Kobayashi are analogous art because they are from the same

field of endeavor of a method and apparatus for processing and authenticating input

information.

Therefore, it would have been obvious to one of ordinary skill in the art at the

invention of time to modify the teaching of Yamaguchi to generate a authentication data,

which in this case are finger prints, that selected by criteria factors m and n, and add the

selecting criteria to the authentication information, same as the inspection information

that are added to its digital data as authentication information that taught by Kobayashi

because therefore the data should be free from alteration and have objectivity, and to

improve the probative value of data as evidence (see Kobayashi page2, line 10-13).

As per **claim 18**, Yamaguchi discloses "an authentication device for

authenticating a physical object, the authentication device comprising" (column 17, line

3-4, Yamaguchi discloses "the embodiment of a fingerprint checking device"): "an input

for receiving a property set Y of a physical object measured using a measurement

procedure" (Figure 1, reference number 1, fingerprint image pickup unit), "and for

receiving a control value V from a storage" (figure 2, reference A11, the control value V

appears to be best finger selection; reference A7 shows the best finger selection has

been stored); "a processor for creating a property set I from the measured property set

Y that meet a predetermined robustness criterion" (Figure 1, reference 10, property set I

appears to be the data that after binarized image converting unit process, and the

robustness criterion appears to be the control variables m or/and n in column 4, line 52-

61), "for creating a property set A from the property set I that includes less information

on the actual properties than property set Y" (property set A appears to be the data after

thinning unit in figure 1. Figure 32 A to B shows the actually thing process of a finger

print. Figure 32 B, the after thinning process picture includes less information than

figure 32 A), "wherein the creating the property set I and the property set A are guided

by a criteria W" (column 4, line 52-61, and figure 1, the block number control variables

m and n control the binarized image converting and, thereafter, the thinning process);

"for generating a control value V' in dependence on properties of the property set A"

(Figure 2, reference number A12, control value V appears to be the best finger

selection. The best fingerprint selection is based on result after thinning process); "and

for authenticating the physical object if there is a predetermined correspondence

between the generated a control value V' and the retrieved control value V and an

output for issuing a signal indicating whether or not the physical object has been

authenticated" (Figure 1, reference 5, "checking unit" and/or "judging unit"; figure 20,

reference number A5, the issued signal appears to be the signal after the process of

match); however, Yamaguchi does not explicitly disclose "receiving a control value V

from a storage including a criteria W".

Kobayashi discloses "inserting the control value V and the criteria W in the

authentication data" (column 16, line 42-49, and Fig. 3, S118-120, control value V

appears to be the authentication information generated after step S116; the criteria W

appears to be the generated inspection information after step S118. Kobayashi

discloses inspection information for inspecting as to whether or not an error is contained

in the digital data is generated. It sets criteria for the authentication data. Kobayashi

also discloses the inspection information is added as further authenticating information

to the digital data), therefore, if the criteria W has been inserted to authentication data

as described above, when retrieving process retrieves "first fingerprint" the inserted

criteria would be retrieved all together.

Yamaguchi and Kobayashi are analogous art because they are from the same

field of endeavor of a method and apparatus for processing and authenticating input

information.

Therefore, it would have been obvious to one of ordinary skill in the art at the

invention of time to modify the teaching of Yamaguchi to generate a authentication data,

which in this case are finger prints, that selected by criteria factors m and n, and add the

selecting criteria to the authentication information, same as the inspection information

that are added to its digital data as authentication information that taught by Kobayashi

because therefore the data should be free from alteration and have objectivity, and to

improve the probative value of data as evidence (see Kobayashi page2, line 10-13).

8.   **Claims 7, 9, 10 and 11** are rejected under 35 U.S.C. 103(a) as being

unpatentable over anticipated by Yamaguchi (US 2001/6314196), in view of Ort et al.

(US 5799098) (hereinafter Ort).

As per **claim 7**, Yamaguchi discloses "the method as described in claim 1", but fails to disclose "wherein the predetermined robustness criterion is based on a signal to noise ratio of the measured properties and the act of creating the property set I includes performing a transformation .GAMMA. on the property set Y to create two disjunct property sets I.sub.1 and I.sub.2 where a signal to noise ratio of properties of the property set I.sub.1 are estimated to be higher than a signal to noise ratio of properties of I.sub.2; and using I.sub.1 as the property set I."

However, Ort discloses the limitations (column 14, line 29-41, Ort uses "filter 110" and "filter 120" to serve the functionalities of transformation Γ. "The two disjunct property set I.sub.1 and I.sub.2" are described as the output data I.sub.FSCE after the process of contrast enhancement in figure 7, reference number 120 and the output data I.sub. FS after the process of low pass filter (Figure 7 reference number 110 respectively. It is obvious for one skilled in the art to observe that I.sub.FSCE has higher Signal to noise ratio than the output data I.sub. FS after the process of low pass filter in Figure 7 reference 110 and the purpose of this transformation is to produce a higher signal to noise ratio.)

Yamaguchi and Ort are analogous art because they are from the same field of using biometric data, which in both applications are fingerprints to enhance the image of fingerprint quality by eliminating the noise, and get a higher signal to noise ratio.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teaching of Yamaguchi to use the low filter and contrast enhancement of Ort because it would provide to enforce the robust criterion, then to

further consolidate the security of the system by applying the techniques to lessen the

contained information in Yamaguchi.

As per **claim 9**, Ort discloses "the method as claimed in claim 7, including the act

of creating the transformation .GAMMA. in dependence on a statistical property of the

measurement procedure" (column 14, line 28-41, Ort discloses the statistical property in

the term of "high frequency noise". The high frequency noise data is obviously

generated during the measurement procedure.)

As per **claim 10**, Ort discloses "the method as claimed in claim 9, wherein the

statistical property includes a covariance matrix derived from estimated properties X of

the object and a corresponding statistical distribution F determined during the

measuring the property set Y" (column 14, line 20-41, Ort discloses estimated

properties X to be "ridge angle", and corresponding statistical distribution F appears to

be "an 800 by 800 pixel image". It is obvious for one skilled in the art that both of the

data sets are represented by matrices. The 800 by 800 pixel image is determined

during the measuring of the original physical object).

As per **claim 11**, Ort discloses "the method as claimed in claim 7, including an

act of deriving a threshold from a noise level in the measured property set and

assigning created properties with an absolute value larger than the threshold to set

I.sub.1" (column 29, line 43-50, with respect to this limitation, Ort discloses "The 256

cells of Q.sub.coarse are filled by sequentially considering the data within each of 256

16.times.16 cell submatrices of Q.sub.smooth that in total comprise all the cells of it.

Each of the 16 cells within a submatrix are examined to determine if the stored cell

value is below a fixed poor quality threshold. If 75% of the cells are below a quality of

0.5 for Q.sub.coarse, then the cell is dubbed as poor quality. If 75% (12 cells) are below

the threshold then: the corresponding Q.sub.coarse (i,aj) is set to 0; otherwise

Q.sub.coarse (i,j) is set to 1." Ort discloses the same concept of deriving a threshold

from the percentage of measured property set by using the term "Q.sub.coarse").

9.   **Claim 8** is rejected under 35 U.S.C. 103(a) as being unpatentable over

Yamaguchi, in view of Ort, and further in view of Vizcaya (Pedro Vizcaya, A personnel

identity verification method using DAB fingerprints (Pattern recognition), 1998)

As per **claim 8**, Yamaguchi and Ort disclose a method as claimed in claim 7 but

do not specifically teach wherein the transformation .GAMMA. is a linear transformation

that converts a vector representing the property set Y to a vector with components as

representing the set I, where each vector component .alpha..sub.i is independent of the

other vector components .alpha..sub.j (j.noteq.i) and wherein the vector components are

sorted according to an estimated signal to noise ratio.

However, Vizcaya discloses "a linear transformation" (Page ix, line 19-23, "a

linear transformation" by "since model is linear, its parameters are efficiently calculated

using standard linear transform techniques. Additionally, the model allows the

evaluation of the specific contribution of each singularity to explain the ridge orientation

everywhere") "that converts a vector representing the property set Y to a vector with

components as representing the set I, where each vector component .alpha..sub.i is

independent of the other vector components .alpha..sub.j (j.noteq.i) and wherein the

vector components are sorted according to an estimated signal to noise ratio" Using

independent vectors with sorted order to represent a physical object (i.e. property set) is well known and expected in the art.

Yamaguchi, Ort, and Vizcaya are all analogous art because they are all from the same field of enhancing the biometric data, which in these three cases specifically fingerprints, by extracting the key feature to get a higher signal to noise ratio, to authenticate an access.

It would have been obvious to one of ordinary skill in the art at the invention time to modify the teaching of Yamaguchi in view of Ort for applying the linear transformation algorithm of Vizcaya because it would provide for the transformation of a vector to the other vectors in more rapid fashion, therefore, to shorten the authentication processing time.

10.   **Claims 12 and 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi in view of Bjorn (US 6035398).

As per **claim 12**, Yamaguchi discloses "the method as claimed in claim 1, wherein the act of creating the control value V" [see rejection to claim 1 above], and "converting each property of the property set A into a binary digit" (transforming a property to binary number representative of whether the property has a positive or negative value is well known technology in the art, for example, US Patent 3,947,876 discloses "to convert the positive and negative data transitions to binary ones and zeros respectively" (see Gary, column 7, line 50-54)), but fails to disclose "includes acts of performing a cryptographic function on properties of the property set A".

However, Bjorn discloses "performing a cryptographic function on a combination of the binary digits" (column 4, line 25-37, and Figure 3, reference number 325, Hash template to create cryptographic key, at block 325, "the template is hashed. For one embodiment, this hash is the cryptographic key. For another embodiment, known techniques are used on the hash to generate the cryptographic key. This cryptographic key is identified with the specific fingerprint, and thus with a specific user". It is known that cryptographic function is performed on combination of the binary code at the invention time).

Yamaguchi and Bjorn are analogous art because they are from the same field of using biometric data to enhance authentication process.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teaching of Yamaguchi to apply the one-way hash function of Bjorn because it would provide to generate a cryptographic key to enhance the security of control value V in Yamaguchi for the authentication.

As per **claim 13**, Bjorn discloses claim 13 "the cryptographic function is a one-way function" (column 4, line 25-37, and Figure 3 reference number 325 Hash template to create cryptographic key, at block 325, the template is hashed. For one embodiment, this hash is the cryptographic key. For another embodiment, known techniques are used on the hash to generate the cryptographic key. This cryptographic key is identified with the specific fingerprint, and thus with a specific user").

Response to Arguments

11.   The applicants amended claims 1, 5, 6, 14, 15, 16, 17, 18. Instead of "helper

data W", it has been amended to "a criteria W". The amendment broadened the scope

of the claim language. The amended limitation was rejected under 35 U.S.C. 103(a) or

35 U.S.C. 102 (b). Please refer to the rejection above to those claims.

12.   On page 28 of the Applicants' Response, the Applicants state Yamaguchi does

not disclose the method that inserting the helper data into the authentication data.

Kobayashi discloses this limitation. Please refer to the rejection above to claims 1-16,

and 18.

13.   On page 29, Applicants argue that for claims 1, 14-17, and 18, Bjorn, Ort, and

Vizcaya do nothing to cure the deficiencies in Yamaguchi; however, the new ground of

rejection presented the limitation was taught by prior arts. Please refer to the rejection

above to claims 1, 14-17, and 18.

14.   From the last paragraph of page 29 to page 31, Applicant's arguments with

respect to claims 1, 14-18, and 2-13 have been considered but are moot in view of the

new ground(s) of rejection.

Conclusion

15.   The Applicants amendment necessitated the new ground(s) of rejection

presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See

MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in

37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to JING SIMS whose telephone number is (571)270-7315.

The examiner can normally be reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JING SIMS/   1/27/2009
Examiner, Art Unit 2437

/J.S./

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437